

Assessing the Privacy Cost in Centralized Event-Based Demand Response for Microgrids

Areg Karapetyan, Syafiq Kamarul Azman, and Zeyar Aung
Department of Electrical Engineering and Computer Science
Masdar Institute of Science and Technology
Abu Dhabi, United Arab Emirates
emails:{akrapetyan, mbinkamarulazman, zaung}@masdar.ac.ae

Abstract—Demand response (DR) programs have emerged as a potential key enabling ingredient in the context of smart grid (SG). Nevertheless, the rising concerns over privacy issues raised by customers subscribed to these programs constitute a major threat towards their effective deployment and utilization. This has driven extensive research to resolve the hindrance confronted, resulting in a number of methods being proposed for preserving customers' privacy. While these methods provide stringent privacy guarantees, only limited attention has been paid to their computational efficiency and performance quality. Under the paradigm of differential privacy, this paper initiates a systematic empirical study on quantifying the trade-off between privacy and optimality in centralized DR systems for maximizing cumulative customer utility. Aiming to elucidate the factors governing this trade-off, we analyze the cost of privacy in terms of the effect incurred on the objective value of the DR optimization problem when applying the employed privacy-preserving strategy based on Laplace mechanism. The theoretical results derived from the analysis are complemented with empirical findings, corroborated extensively by simulations on a 4-bus MG system with up to thousands of customers. By evaluating the impact of privacy, this pilot study serves DR practitioners when considering the social and economic implications of deploying privacy-preserving DR programs in practice. Moreover, it stimulates further research on exploring more efficient approaches with bounded performance guarantees for optimizing energy procurement of MGs without infringing the privacy of customers on demand side.

Index Terms—Demand response, differential privacy, microgrids, privacy preserving energy management, randomized response.

I. INTRODUCTION

Rising environmental and economic concerns necessitate modernization of the aging power grid infrastructure into a more sustainable and optimized cyber-physical system, SG. Microgrids, reckoned as a vital contributor towards this transition, facilitate large scale deployment of renewable Distributed Generation (DG) and incorporation of new load types such as plug-in hybrid electric vehicles (PHEVs). However, the volatile nature of renewable energy sources along with increasing customer expectation for both power quality and quantity further complicate the energy management of MGs besetting with an intricate power allocation problem critical for maintaining system stability.

DR management has proven instrumental in resolving the problem confronted, offering efficient schemes for energy procurement and optimization of MGs suffering from power

disbalance [1]. To achieve the desired system reliability, resilience and power quality, DR programs aim at establishing a mutually beneficial interaction framework for DR participants and aggregators where power generation drives the demand. With DR, customers are incentivized to shape and schedule their consumption profiles to flatten the peak demand, consequently deferring the cost of generation expansion and ancillary grid services. Among other advantages, DR enables reduced price variations [2], enhanced congestion management [3] and strengthened system security [4]. DR programs can be broadly categorized into two classes, price-based and event-based [5]. Event-based DR programs are efficient especially during the times when there is insufficient supply of power on MG side to meet the available demand [5], [6].

Increasing customer participation translates into elevated benefits for DR operators, as the availability and volume of controllable load reserves grows with the number of DR participant devices. To this end, customers' concerns over privacy could constitute a major threat [7], [8]. DR programs with centralized control architecture, which are commonly deployed in practice [9], [10], entail information pertaining to customer loads and preferences as the inputs for optimization. This may limit customer participation severely since customers may not be willing to reveal such information out of confidentiality reasons [11]. Possessing knowledge on the desired power valuation (utility) and electricity consumption characteristics of a customer empowers DR operators or potential eavesdroppers to exploit this marketable information to their own benefit. According to [12], information on power consumption alone suffices to infer customer's appliances operated or even daily activities. More importantly, with this information an adversary participant may attempt to manipulate the DR outcome by misreporting own utility value for the sake of profit.

It is widely acknowledged that ad-hoc approaches such as anonymizing customer data are devoid of privacy features owing to the availability of public side information [13]. Conversely, it might be tempting to retain privacy in DR with a distributed control scheme in place, where response decisions are computed on a customer's end involving exchange of surrogate information only. In [14] a distributed energy management strategy is proposed with the objective of maximizing aggregate utilities of the appliances in the households and minimizing power losses. However, distributed

DR programs typically suffer from synchronization problems and could incur diminished system-wide controllability and efficiency, in contrast to the centralized ones [9]. Besides, it is suspected that, in general, inferring the private customer information concealed implicitly in the exchanged surrogate coordination signals could be still viable. In the view of the above arguments, deriving efficient privacy-aware strategies for solving large-scale DR problems under centralized control philosophy becomes vital.

While ensuring customer privacy, DR operators should also seek to achieve certain benefits determined by the objective function of DR optimization problem. As long as the private information lies in the objective function or constraint matrix of the DR problem these two objectives are conflicting. Indeed, optimizing the DR management choosing to ignore customer input data as a privacy-preventive measure may lead to arbitrarily worse solutions when compared to the optimal solution. The induced suboptimality gap typifies the cost of privacy, in a sense to be formalized in Section IV. Most of the extant literature on energy management of MGs, such as [11], [15], [16] and [17]–[19], approach this trade-off from one angle or the other leaving the privacy cost largely unexamined. Among these works, those dealing with the privacy aspect advocate approaches relying on cryptographic techniques and security protocols that may evoke substantial communication and computation overhead, thereby questioning their practicality in large-scale applications.

Recently, smart metering infrastructure sparked considerable research efforts [20]–[23] in response to privacy threats. Various schemes have been developed for securing the smart meter data aggregation and customer demand reporting in SG. However, the setting in these studies envisions smart metering primarily in the scope of electricity billing service rather than deployed within a DR optimization model as in the case studied here. A simple yet effective privacy solutions are presented in [24], [25] for demand reporting by utilizing rechargeable batteries. Essentially, the batteries are used as a proxy between smart metering devices and household appliances to mask consumer demands in a non-intrusive manner. This is desirable as it maintains consumer privacy without introducing additional noise while satisfying smart grid constraints.

Against this background, the focus here is to explore the interplay between privacy and optimality in centralized event-based DR management programs through extensive empirical analysis. In addition to this, the gap between suboptimal private and optimal non-private solutions is bounded theoretically. We further unravel the obscure relationship between privacy and DR parameters driving this trade-off, thus conducting to deeper understanding of the scales and dynamics of privacy phenomena in event-based energy management for MGs.

As to other related literature, studies in [26], [27] covered a more thorough investigation of the privacy cost. An efficient privacy-assuring metering scheme is proposed in [26]. Customer's privacy is achieved by adding a randomly

generated number to the measurement sent from the smart meter to the power provider, making it a simple and low complexity approach. The trade-off between economic benefit and privacy is evaluated in terms of the error in the billed amount to SG operator. Compared to [26], this paper provides a deeper insight of the privacy effect on MG performance when evaluating it within a comprehensive DR optimization framework with an accurate realistic MG model and privacy levels adaptable to customer preferences. Privacy preservation is also evident in economic load dispatch control problem for minimizing generation cost [27]. Customer demands are altered by noise prior to reaching the control unit to enable the privacy. The increased generation cost attributed to privacy is assessed through small scale experiments based on a 5-bus power system with 200 customers only and a simplified grid model that omits AC power flow equations.

Typically, in a DR management scheme, there is a single load-serving entity (LSE) or an operator of MG, who coordinates the decisions of DR participants. There is a high probability that an MG once initiated will be short of power, consequently resulting in significant voltage and frequency deviations, and leading to its instability. The LSE then invokes the featured event-based DR program to ensure the endurance of an MG by balancing out power generation and demand. Constrained by the net available apparent generation and power flow equations, LSE is required to make control decisions in real time as to maximize the total utility of satisfied customers without violating their privacy. To attain this in a scalable fashion, an efficient privacy-preserving mechanism introduced in [28] is leveraged to this end, which also provides a definite theoretical guarantee on the level of privacy and optimality. The privacy cost is quantified by benchmarking the maximized utility of this mechanism with that in the omniscient case, where customer privacy is not protected.

The major contribution of this preliminary study is centered on two salient features that differentiate it from the surveyed literature. First, particular emphasis is paid to establishing a realistic DR system with an accurate and reliable MG model capturing power flow and operational constraints (e.g., Kirchhoffs law, voltage bounds, reactive power) associated with the underlying distribution network. The importance and necessity of this were acknowledged in [29]–[31], which highlight that using a simplified MG model may lead to infeasible load management decisions in practice and thus impairs the credibility of the results produced. Second, power valuation, which is a core design parameter of an event-based DR, is regarded as information private to an individual customer only. While various approaches were proposed for tackling privacy in demand reporting (e.g., the method in [24], [25] relying on rechargeable batteries), the setting with private power valuations has not been studied properly. Taken together, these contributions illustrate and appraise the ramifications of deploying event-based DR programs in practice where privacy concerns are a priority.

As one demonstration, the proposed privacy-preserving DR scheme is applied to a 4-bus feeder from Canadian distribution

system (see Fig. 1 in Section III). The results indicate that incorporating privacy in centralized event-based DR management may degrade the optimality of the produced load management decisions severely. Nevertheless, considering a realistic scenario with heterogeneous privacy levels varying among customers may smooth the impact of privacy. Also, it is inferred that the privacy cost is influenced by several DR parameters including customer type, power valuation and privacy level.

II. PRELIMINARIES

This section briefly scopes preliminaries of the adopted privacy notion.

A. Differential Privacy

When it comes to quantifying the extent of privacy of a customer participating in DR program, this paper adheres to the notion of *differential privacy*. Originated from the research in [32] and defined by [33], differential privacy has evolved as a rigorous definition of privacy in computer science. As such, it can be interpreted as a guarantee that altering an individual record in the input set does not impact the distribution of the computation outcomes significantly. In other terms, customers' private information becomes indistinguishable in the output of a differentially private algorithm. This yields a strong privacy guarantee regardless of any auxiliary information the adversary may possess.

On the other hand, it is increasingly hard to derive efficient algorithms meeting such a stringent privacy guarantee [28]. As a consequence, many fundamental problems as those studied in [34], [35] have private solutions, while lacking efficient algorithms. For a certain class of combinatorial optimization problems several approximation algorithms are devised in [36] that retain differential privacy. *Laplace mechanism* and *exponential mechanism*, which by far are the most prevalent approaches practiced for differential privacy were introduced in [33] and [37], respectively. Unlike the former one, exponential mechanism runs in linear time of its output range, which might largely outweigh the number of customers, and thus is not suitable for the purposes of this study.

The framework of differential privacy represents information private to a customer as a set D referred to as *database*. Let \mathcal{D} be the domain of all databases of interest. The basic idea underlying this framework is to draw an association between privacy and impact of an individual customer in the database. The impact, that is, changes that occur in the database when altering or deleting a customer's record is characterized by the concept of *neighboring databases*. Define databases $D \in \mathcal{D}$ and $D' \in \mathcal{D}$ to be neighboring if they are identical except a single record. Differential privacy is formalized by the definition below.

Definition 1 (Differential privacy [33]). *A randomized algorithm $\mathcal{A} : \mathcal{D} \rightarrow \mathbb{R}^n$ that maps databases to an output range \mathcal{R} is (ϵ, δ) -differentially private if for every pair of neighboring databases $D \in \mathcal{D}$, $D' \in \mathcal{D}$ and $\forall S \subseteq \mathcal{R}$*

$$Pr[\mathcal{A}(D) \in S] \leq e^\epsilon \cdot Pr[\mathcal{A}(D') \in S] + \delta, \quad (1)$$

where $\epsilon > 0$ and $\delta \in [0, 1)$.

Similarly, an algorithm \mathcal{A} is called ϵ -differentially private, if $\delta = 0$. The level of privacy is characterized by the constant ϵ . The smaller the ϵ the higher is privacy level.

III. SYSTEM MODEL AND ASSUMPTIONS

Towards defining the proposed DR optimization problem formally, this section starts by modeling the system and its components. The adopted DR model envisions a single LSE procuring the responses of customers' demands over a decision horizon $\mathcal{T} \triangleq \{1, \dots, m\}$. The decision horizon \mathcal{T} is discretized into m equal periods with a duration corresponding to the required time resolution granularity at which DR management decisions are to be produced. At each time slot $t \in \mathcal{T}$, the net available generation capacity of MG is denoted by $C_t \in \mathbb{R}_+$.

A. Load Model

Consider a set of customers $\mathcal{N} \triangleq \{1, \dots, n\}$ for a DR management scheme run by LSE. A customer $k \in \mathcal{N}$ is associated with a complex-valued power demand $S_k \in \mathbb{C}$ required for operating certain electric appliances at particular time instant. Denote by $S_k^R \triangleq \text{Re}(S_k)$ the *active power* demand of customer k , and by $S_k^I \triangleq \text{Im}(S_k)$ the *reactive power* demand. For clarity of presentation, this paper assumes (via a rotation of power demand vectors) that $S_k^R \geq 0$ and $S_k^I \geq 0$ for $\forall k \in \mathcal{N}$.

To allow effective DR application, diverse customer appliances should be taken into account. The customers' demands here are categorized into two types according to their operation and energy consumption characteristics, *elastic* (divisible) and *inelastic* (indivisible). The demand of a customer possessing inelastic load can be either shed or fed completely. This models the electric appliances that can operate only under particular energy supply level (e.g., washing machine, vacuum cleaner). Different from the inelastic demands, an elastic load may be satisfied partially and adjusted to operate with different energy consumption levels (e.g., air conditioner, LED light).

B. Modeling the Distribution Network

To incorporate the power flow and voltage constraints into the DR optimization problem a model of the distribution network, resembling that of in [38], is established below. We shall confine our attention to radial (tree) distribution networks which are common in practice [39].

The distribution system is represented by a graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, where each customer $k \in \mathcal{N}$ is located at a given node except the root. The set of nodes \mathcal{V} denote the electric buses, whereas the set of edges \mathcal{E} denote the distribution lines. The nodes in \mathcal{V} are indexed by $\{0, 1, \dots, |\mathcal{V}|\}$, where the node 0 denotes the generation source of MG. Let $V_i \in \mathbb{C}$ denote the voltage of node $i \in \mathcal{V}$. Define $I_{i,j}$ to be the current flowing through edge $e = (i, j) \in \mathcal{E}$ and with a slight abuse of notation, $\tilde{S}_{i,j} \in \mathbb{C}$ to be the transmitted power through that edge. Similarly, let $z_{i,j} \in \mathbb{C}$ be the impedance of that edge. Denote by $v_i \triangleq |V_i|^2$ and $\ell_{i,j} \triangleq |I_{i,j}|^2$ the magnitude square

of voltage and current, respectively. For each node $i \in \mathcal{V} \setminus \{0\}$, there is a set of customers attached to i , denoted by \mathcal{M}_i .

A power flow in a steady state can be characterized by a set of power flow equations. In radial networks (which include paths) the Branch Flow Model (BFM) proposed by [40] can be used to model them. Assuming v_0 is given, the BFM is captured by the following set of equations for $\forall (i, j) \in \mathcal{E}$

$$\ell_{i,j} = \frac{|\hat{S}_{i,j}|^2}{v_i}, \quad (2)$$

$$v_j = v_i + |z_{i,j}|^2 \ell_{i,j} - 2\text{Re}(z_{i,j}^* \hat{S}_{i,j}), \quad (3)$$

$$\hat{S}_{i,j} = \sum_{l:(j,l) \in \mathcal{E}} \hat{S}_{j,l} + \sum_{k \in \mathcal{M}_j} S_k x_k + z_{i,j} \ell_{i,j}, \quad (4)$$

where x_k is the load management decision produced by LSE for customer $k \in \mathcal{N}$, $\text{Re}(\psi)$ denotes the real component of a complex number $\psi \in \mathbb{C}$ and ψ^* denotes the complex conjugate of ψ . Decision variable x_k takes values either from $[0, 1]$ or $\{0, 1\}$ for elastic and inelastic demands, respectively. Equations (2) - (4), essentially, capture Ohm's law combined with the Kirchhoffs laws of electric flows and power flow definitions.

Furthermore, for each node $i \in \mathcal{V} \setminus \{0\}$ the following operational constrain should be satisfied

$$v_{\min} \leq v_i \leq v_{\max}, \quad (5)$$

where $v_{\min}, v_{\max} \in \mathbb{R}^+$ are the minimum and maximum allowable voltage magnitude square at any node, respectively. The setting studied here assumes a limited apparent power generation on MG and thus at each time step $t \in \mathcal{T}$

$$|\hat{S}_{0,1}| \leq C_t. \quad (6)$$

Observe that BFM model is non-convex due to the quadratic equality constraints in Eqn.(2) and thus is computationally intractable in general. We therefore consider relaxing them to inequalities in Eqn. (7) to convexify the model. Due to the same reason, this relaxation is adopted in [29], [30], [41]. Obviously, when the equality in (7) is attained then the relaxation is exact. In fact, it was shown in [42] that this relaxation happens to be exact under certain mild conditions in most of the practical radial distribution systems including IEEE bus systems.

$$\ell_{i,j} \geq \frac{|\hat{S}_{i,j}|^2}{v_i}, \quad \forall (i, j) \in \mathcal{E} \quad (7)$$

Lastly, it is assumed that the MG system encompasses a hybrid mix of traditional and renewable energy (RE) supplies that could collectively have a variable (depending on the availability of RE and storage available) yet dispatchable capacity. In the sequel, using the established distribution model, the employed differentially private mechanism of [28] is applied to a 4-bus feeder of the Canadian benchmark system depicted in Fig. 1.

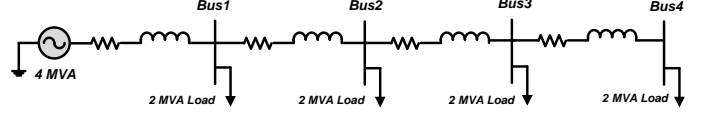


Fig. 1: A 4-bus feeder from Canadian benchmark distribution system.

C. Customer Preference Model

In a DR program where each subscribed customer is an independent decision maker, typically, the response to the incentives by the DR aggregator is modeled by an *utility function*. The response may vary depending on the particular time of a day (e.g. at peak and non-peak hours). Moreover, it may vary from customer to customer based on the consumption profile (i.e., when considering *residential* and *commercial* customers).

To simplify the exposition, the utility function is summarized by an *utility value* (power valuation) u_k^t associated with a customer $k \in \mathcal{N}$. This value quantifies the extent of satisfaction obtained (or alternatively, the payment) by customer k when own power demand is satisfied at time $t \in \mathcal{T}$. In the case with inelastic demands, if S_k is satisfied at time slot t , u_k^t is the perceived utility for customer k , otherwise zero utility is perceived. As for a customer $k' \in \mathcal{N}$ with an elastic load, a portion $b \in [0, 1]$ of the power demand $S_{k'}$ drawn from MG at time instant t imparts an utility of $b \cdot u_{k'}^t$.

D. Privacy-Preserving DR

Recall that the DR scheme under study requires protecting customer sensitive information in the input data. In particular, this paper focuses on the case where utilities, which define the objective function of DR optimization problem, are the sensitive information to customers. In more detail, the private database at time t of the participating customers is $D = \{u_k^t\}_{k \in \mathcal{N}}$. Since only aggregate power demands are required by LSE, it is assumed that the customer loads can be protected in a non-intrusive manner by a method akin to those proposed in [24], [25] relying on rechargeable batteries. In a sense, shifting between neighboring databases affects only the objective function of the DR problem leaving the constraint matrix unchanged.

In the envisioned DR program featuring a centralized control scheme, each customer declares his reactive and active power demand through the equipped smart metering infrastructure to LSE upon request. In order to prevent customer utilities from being exposed to LSE or a potential eavesdropper the adopted strategy produces a perturbed utility value to obfuscate customer's true valuation. Section IV scopes a detailed explanation of this mechanism and provides provable guarantees on its privacy level.

It is worthy to note, that this scheme is general enough to handle customers with multiple utilities (independent of each other) for corresponding subsets of own demands. This allows customers to prioritize their demands based on the importance and value without altering the proposed problem

formulation. To effectively control DR management, low-latency communication infrastructure between the LSE and customers using separate power supply will be utilized in the proposed scheme. Such an infrastructure is enabled by the standards of SG communication protocols [43]. Additionally, it is to be assumed that LSE has full control over the on/off or adjusting operations of its customers' demands.

As mentioned previously, devising computationally efficient algorithms in differential privacy with provable optimality guarantees is substantially difficult. In fact, it was shown in [28] that if one makes no assumptions on the sensitivity of the private data it is impossible to devise such an algorithm with non-trivial optimality guarantees. This necessitates the need for introducing the simplifying assumption stated hereunder that will be followed throughout this paper.

Assumption 1. *There exist positive u_{\max} and u_{\min} known to LSE apriori such that for $\forall k \in \mathcal{N}$, $u_{\min} \leq u_k^t \leq u_{\max} \quad \forall t \in \mathcal{T}$.*

We remark that Assumption 1 naturally holds in DR systems, since usually u_{\min} and u_{\max} are determined by LSE. The subsequent section defines the DR optimization problem and formalizes the privacy cost.

IV. PROBLEM FORMULATION AND CHOSEN APPROACH

A. Optimization Problem

Now that the system model is established, the *utility maximizing demand response problem* (UMDR) at time $t \in \mathcal{T}$ can be formulated in an optimal power flow framework by the following *quadratically constrained mixed integer programming* (QCMIP) problem.

$$\begin{aligned} \text{(UMDR)} \quad & \max_{x_k, v_i, \ell_{i,j}, \hat{S}_{i,j}} \sum_{k \in \mathcal{N}} u_k^t x_k \\ \text{subject to} \quad & (3), (4), (5), (6), (7) \end{aligned} \quad (8)$$

$$x_k \in \{0, 1\}, \quad \forall k \in \mathcal{N} \quad (9)$$

Here, x_k is a binary decision variable that takes value 1 if and only if the k -th customer's power demand S_k is satisfied and 0 otherwise. The UMDR problem aims at maximizing the overall net utility of customers while maintaining the apparent power generation C_t bound at time instant $t \in \mathcal{T}$, power flow equations and voltage levels.

Evidently, UMDR is NP-HARD, since the 0-1 classical knapsack problem is its special case. Relaxing binary (discrete) decision variables (x_k) to continuous ones in UMDR problem, such that $x_k \in [0, 1]$, yields a *convex quadratic programming* problem denoted by UMDR_L. This seemingly small change in problem formulation, in fact, alters the complexity of DR optimization problem notably, since the convex variant can be solved optimally in polynomial time (e.g., by applying Interior Point methods). Aside from complexity, setting the decision variable (x_k) to be discrete or continuous alters the practical aspects of DR application. Concretely, the continuous case corresponds to customers having only elastic power demands. As for the case with binary decision variables, DR participant demands comprising the customer set are solely inelastic loads.

B. Differentially Private Method

This subsection presents an efficient randomized mechanism, introduced by [28], to compute solutions of UMDR and UMDR_L problems privately. The method relies on a principle differential privacy technique which is explained in what follows.

Define a function $f : \mathcal{D} \rightarrow \mathbb{R}^n$ to be Δ -sensitive if $\|f(D) - f(D')\|_1 \leq \Delta$ for \forall neighboring $D, D' \in \mathcal{D}$. Let $\text{Lap}(\Omega)$ denote the Laplace transformation of Ω with a probability density function $f(x | \Omega) = \frac{1}{2\Omega} e^{-\frac{|x|}{\Omega}}$. Then, applying the Laplace mechanism to a Δ -sensitive function $f(D)$ yields $f(D) + [\mu_1, \mu_2, \dots, \mu_n]^T$, where $\mu_1, \mu_2, \dots, \mu_n$ are n independent and identically distributed draws from $\text{Lap}(\frac{\Delta}{\epsilon})$ with $\epsilon > 0$.

Theorem 1 ([44]). *A randomized algorithm \mathcal{A} that invokes the Laplace mechanism explained above is ϵ -differentially private.*

Instead of releasing the true customer valuations, the considered mechanism perturbs each customer's utility u_k^t independently by adding a noise drawn from the Laplace distribution that commensurates with the desired level of privacy. Define $\hat{u}_k^t \triangleq u_k^t + \text{Lap}(\frac{(u_{\max} - u_{\min})\sqrt{8n \log(\frac{1}{\delta})}}{\epsilon})$ to be the perturbed utility of customer $k \in \mathcal{N}$ at time $t \in \mathcal{T}$. Then the private analog of UMDR_L problem (DR with elastic demands) is embodied by the following *convex programming problem*.

$$\begin{aligned} \text{(UMPDR)}_L \quad & \max_{x_k, v_i, \ell_{i,j}, \hat{S}_{i,j}} \sum_{k \in \mathcal{N}} u_k^t x_k \\ \text{subject to} \quad & (3), (4), (5), (6), (7) \end{aligned} \quad (10)$$

$$x_k \in [0, 1], \quad \forall k \in \mathcal{N} \quad (11)$$

Solving UMPDR_L problem non-privately results in a private solution to the original one. Note that any feasible solution to UMPDR_L is also feasible for UMDR_L. Denote by $X_L^* \subseteq \mathcal{N}$ an optimal solution of UMDR_L and by $\text{OPT}_L \triangleq \sum_{k \in X_L^*} u_k^t$ the corresponding total utility for any time $t \in \mathcal{T}$. Set $\hat{X}_L^* \subseteq \mathcal{N}$ to be an optimal solution of UMPDR_L and define $\text{OPT}_L^{\text{DP}} \triangleq \sum_{k \in \hat{X}_L^*} u_k^t$.

Theorem 2 ([28]). *An optimal solution \hat{X}_L^* for UMPDR_L problem is (ϵ, δ) -differentially private feasible solution to UMDR_L that with high probability satisfies the following additive optimality bound $\text{OPT}_L^{\text{DP}} \geq \text{OPT}_L - \alpha$ where $\alpha = \frac{4(u_{\max} - u_{\min})\sqrt{8n \log(\frac{n}{\delta})}}{\epsilon}$.*

The proof of Theorem 2 can be consulted in [28].

The privacy cost in this study is defined in terms of the relative difference between OPT_L and OPT_L^{DP} . In a sense, it exemplifies the diminished objective value arising as a result of solving the DR optimization problem with inaccurate customers demands obfuscated by differentially private noise. For UMDR_L, the cost of privacy, denoted by $\Phi_L \in [0, 1]$, is defined as

$$\Phi_L \triangleq \frac{\text{OPT}_L - \text{OPT}_L^{\text{DP}}}{\text{OPT}_L}. \quad (12)$$

When $\Phi_L = 0$, this represents the ideal desirable case when no cost is incurred on the optimality of the produced energy management decisions. The closer Φ_L to 1 the higher the privacy cost is and so is the optimality gap. For example, $\Phi_L = 0.4$ implies that incorporating the privacy-preserving method entails 40% loss of optimality. Following the logic of Eqn. (12), define Φ to be the privacy cost for UMDR problem.

V. EMPIRICAL EVALUATION

To complement the analytic result in Theorem 2, this section evaluates the utilized differentially private mechanism empirically by applying it to a simulated 4-bus feeder from Canadian benchmark distribution system, which appears in Fig.1. The objective is to investigate and quantify the privacy cost in the proposed event-based DR system. The CPLEX optimizer is utilized to obtain the close-to-optimal solutions numerically for UMDR, UMDR_L problems and their differentially private analogs.

A. Simulation Setup and Settings

The feeder, which is rated at 8.7MVA, 400A and 12.47KV, is simulated with an overall generation capacity of 4MVA and over 1500 customers allocated among the nodes. Each feeder section is a 700MCM Cu XLPE cable with impedance $z = 0.1529 + j0.1406 \Omega/km$. Each customer has a specific power demand (including both active and reactive power) and a utility that is generated according to a probability preference model. Due to limited power supply, the customers may suffer from a reduction of generation capacity occasionally. Various types of loads are considered including *residential* and *commercial* customers. Typically, the load power factor varies between 0.8 to 1 (to comply with IEEE standards) and thus the maximum phase angle between any pair of demands is restricted to be in the range of $[0, 36^\circ]$.

B. Case Studies

Various case studies are performed to evaluate the studied privacy-preserving mechanism considering diverse scenarios with respect to the correlation between customer loads and utilities, consumption profile and privacy levels. The following are settings for the case studies in this paper.

(i) Utility-demand correlation:

- Quadratic utility (Q):** The utility of a customer is a quadratic function of the power demand in the form of $u_k^t(|S_k|) = a \cdot |S_k|^2 + b \cdot |S_k| + c$, $\forall t \in \mathcal{T}$, where $a > 0, b, c \geq 0$ are predetermined constants.
- Uncorrelated setting (U):** The utility of each customer is independent of the power demand and is generated randomly from $[0, |S_{\max}(k)|]$, where $|S_{\max}(k)|$ depends on the customer type.

(ii) Customer types:

- Residential (R) customers:** The customer set is comprised of residential customers having small power demands ranging from 1500VA to 15KVA.
- Mixed (M) customers:** The customer set is comprised of a mix of commercial and residential customers.

Commercial customers have big power demands ranging from 300KVA up to 1MVA and constitute no more than 10% of all customers chosen at random.

(ii) Privacy levels:

- Fixed (F) privacy level:** Customers are assigned only a single homogeneous level of privacy predetermined by LSE.
- Variable (M) privacy level:** Customers are allowed to choose the desired privacy protection level from a predefined set offered by LSE.

In this paper, the case studies will be represented by the aforementioned acronyms. For example, the case study named QMV stands for the one with mixed customers, quadratic utility-demand correlation and heterogeneous privacy levels.

C. Simulations with Homogeneous Privacy Levels

In this subsection the privacy cost is evaluated for case studies with homogeneous privacy levels, where each case study is analyzed considering changes in the set of customers. For each DR optimization problem (i.e., UMDR and UMDR_L), two different privacy levels are examined where the corresponding value of ϵ is set to 0.01 and 1. As for additive privacy parameter δ , the value is fixed to 0.5 for all case studies.

The privacy cost for UMDR is compared for different values of ϵ in Fig.2. The employed privacy method with an input parameter of ϵ is applied to the UMDR problem (i.e., this corresponds to solving UMPDR with perturbed customer utilities calculated accordingly) 30 times for each of the m number of customers, where m varies between 500 to 1500 in steps of hundred. For case studies with residential customers, m varies between 1000 to 1500 since with fewer customers the total load on MG is less than the supply thus resulting in trivial DR decisions. Each of 30 iterations yields random changes in demands and utilities of customers.

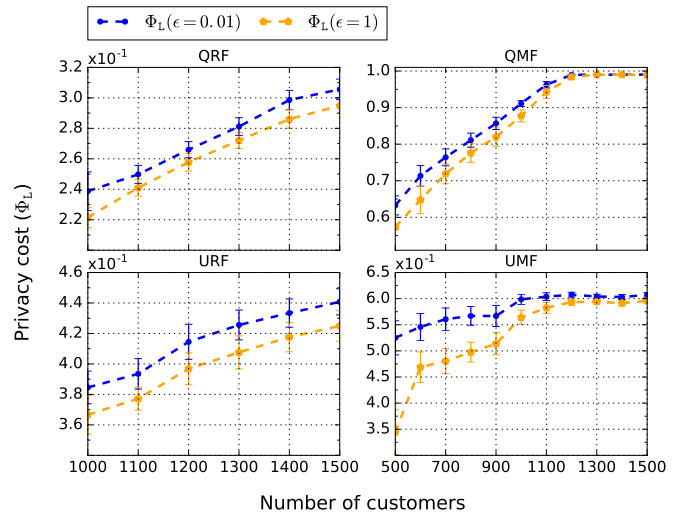


Fig. 2: The average privacy cost for UMDR_L against the number of customers at 95% confidence interval.

The privacy cost for UMDR is contrasted with that of UMDR_L in Fig. 3 considering a fixed number of customers. Here, the privacy level ϵ is varied from $5 \cdot 10^{-5}$ to 1 for 900 customers considering random changes in demands and utilities.

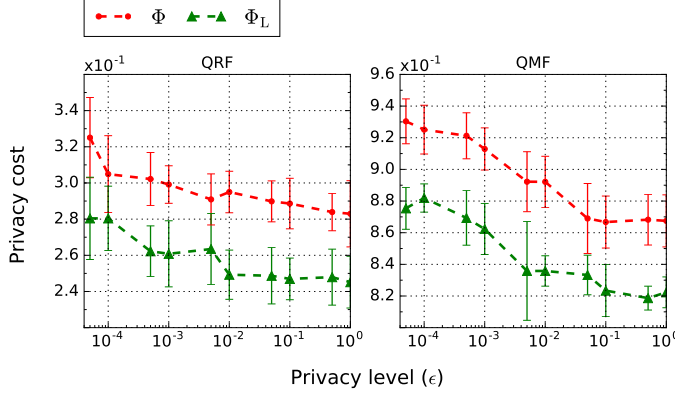


Fig. 3: The average privacy cost for UMDR and UMDR_L against ϵ at 95% confidence interval.

One of the important findings observed is a common trend appearing in all the case studies performed. As can be inferred from Figures 2 and 3 increasing ϵ reduces the optimality gap and hence the privacy cost. In other terms, the lower the level of privacy the higher the privacy cost. This directly implies that the privacy cost increases with the noise magnitude since the Laplace noise added to each customer's utility increases when lowering ϵ . As illustrated in Fig. 2, on a MG with 500 customers the studied privacy preserving mechanism resulted in a privacy cost of 0.59 when $\epsilon = 1$ (i.e., the optimality of DR is decreased by 59%), whereas when $\epsilon = 0.1$ the privacy cost is about 0.63, considering the case study QMF.

Another important observation is that with increasing customer participation optimality of produced DR solutions degrades drastically. As depicted in Fig. 2, when the number of customers is small the privacy cost is only in order of 0.6 when considering case study QMF, while as the customer set cardinality grows privacy cost proliferates approaching nearly 1. This highlights the necessity of devising efficient privacy preserving mechanisms, with a constant factor guarantee on the optimality gap, capable of solving large-scale DR management problems.

Also, it is observed that the privacy cost is sensitive to different customer types. In particular, the privacy cost grows slower for case studies with residential customers than in those with mixed industrial and residential customers. As indicated in Fig. 2, the difference in privacy cost for case study QRF is about 0.08 when considering the number of customers ranging from 1000 to 1500. In contrast, for the same range the privacy increases nearly by 1.2 in case study QMF. In a sense, incorporation of privacy has more significant degrading effect on the optimality for the scenarios with mixed customers as compared to those with only residential customers.

D. Dynamic Generation Capacity and Heterogeneous Privacy Levels

The previous set of experiments considered an MG with a fixed generation capacity and homogeneous privacy levels. Here simulations are performed considering the case when the MGs generation capacity is varying over time, which could be representative of a case of hybrid system with renewable DG sources. Furthermore, in a real-world situation customers may desire different levels of privacy depending on their preferences. Thus, the simulation studies performed in this section consider heterogeneous privacy levels.

The time-varying generation capacity of MG that follows a Bernoulli process is dynamically varied between 1MVA and 4MVA from time 0 to 10000 (seconds). To analyze the effect of heterogeneous privacy levels, the employed mechanism is applied to the feeder with 1000 customers. The observed privacy cost is plotted in Fig 4.

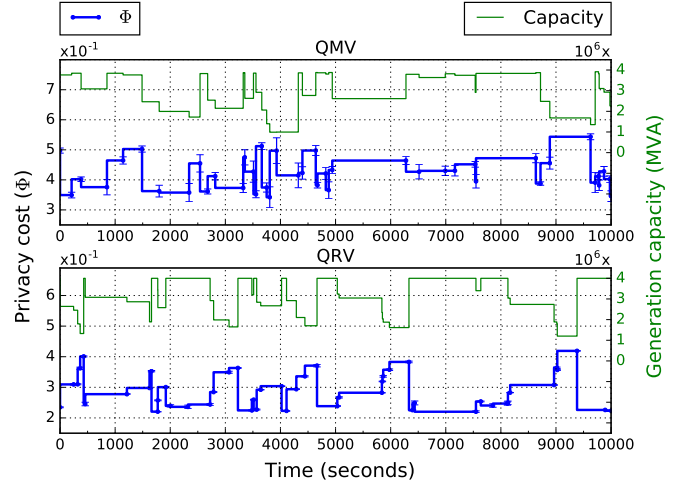


Fig. 4: The average privacy cost against the number of customers at 95% confidence interval considering dynamic generation capacity.

The privacy cost and absolute noise magnitude (per customer), which appear in Fig. 5, are evaluated considering changes in the number of customers, whereas MG generation capacity remains fixed.

The results demonstrate that allowing flexible privacy levels, instead of flat ones, may considerably increase the optimality of the proposed DR management scheme. The average privacy cost plotted in Fig. 5 for case study QMV fluctuates around 0.4 while the number of customers changes and does not drift far away from that threshold. Whereas, in the scenarios with homogeneous privacy levels appearing in Fig. 2 the privacy cost was sometimes as high as nearly 1.

VI. CONCLUSION

This paper studies the trade-off between privacy and optimality in centralized DR management of MGs. Under the framework of differential privacy, the privacy cost is quantified empirically through extensive numerical simulations on a

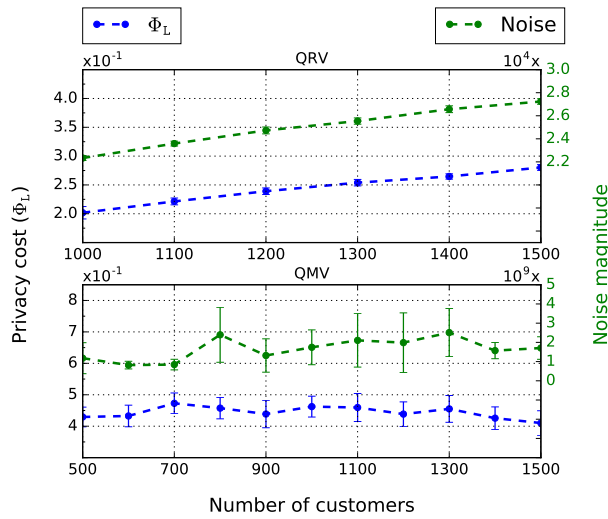


Fig. 5: The average privacy cost as a function of the number of customers at 95% confidence interval.

realistic distribution network. The observed results illustrate the striking effect posed on the optimality of produced solutions to DR optimization problem when considering increased privacy guarantees. According to the findings, the optimality gap approaches nearly 90% in some cases, which urges the need for efficient privacy preserving algorithms with constant theoretical guarantees on the worst case performance. The major factors identified in this study that define this trade-off are the customer utility function, privacy level and customer type.

REFERENCES

- [1] F. Rahimi and A. Ipakchi, "Demand response as a market resource under the smart grid paradigm," *IEEE Transactions on Smart Grid*, vol. 1, pp. 82–88, June 2010.
- [2] C.-L. Su and D. Kirschen, "Quantifying the effect of demand response on electricity markets," *IEEE Transactions on Power Systems*, vol. 24, pp. 1199–1207, Aug 2009.
- [3] A. Khodaei, M. Shahidehpour, and S. Bahramirad, "Scuc with hourly demand response considering intertemporal load characteristics," *IEEE Transactions on Smart Grid*, vol. 2, pp. 564–571, Sept 2011.
- [4] Y. Wang, I. Pordanjani, and W. Xu, "An event-driven demand response scheme for power system security enhancement," *IEEE Transactions on Smart Grid*, vol. 2, pp. 23–29, March 2011.
- [5] P. Siano, "Demand response and smart grids survey," *Renewable and Sustainable Energy Reviews*, vol. 30, pp. 461–478, 2014.
- [6] W. Chen, X. Wang, J. Petersen, R. Tyagi, and J. Black, "Optimal scheduling of demand response events for electric utilities," *IEEE Transactions on Smart Grid*, vol. 4, pp. 2309–2319, Dec 2013.
- [7] R. Hoenkamp, G. B. Huitema, and A. J. de Moor-van Vugt, "Neglected consumer: The case of the smart meter rollout in the netherlands, the," *Renewable Energy L. & Pol'y Rev.*, p. 269, 2011.
- [8] A. Molina-Markham, P. Shenoy, K. Fu, E. Cecchet, and D. Irwin, "Private memoirs of a smart meter," in *Proceedings of the 2Nd ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Building*, BuildSys '10, (New York, NY, USA), pp. 61–66, ACM, 2010.
- [9] S. Lu, N. Samaan, R. Diao, M. Elizondo, C. Jin, E. Mayhorn, Y. Zhang, and H. Kirkham, "Centralized and decentralized control for demand response," in *ISGT 2011*, pp. 1–8, Jan 2011.
- [10] J. S. Vardakas, N. Zorba, and C. V. Verikoukis, "A survey on demand response programs in smart grids: Pricing methods and optimization algorithms," *IEEE Communications Surveys Tutorials*, vol. 17, pp. 152–178, Firstquarter 2015.
- [11] Y. Gong, Y. Cai, Y. Guo, and Y. Fang, "A privacy-preserving scheme for incentive-based demand response in the smart grid," *IEEE Transactions on Smart Grid*, vol. 7, pp. 1304–1313, May 2016.
- [12] J. Zhao, T. Jung, Y. Wang, and X. Li, "Achieving differential privacy of data disclosure in the smart grid," in *IEEE INFOCOM 2014 - IEEE Conference on Computer Communications*, pp. 504–512, April 2014.
- [13] A. Narayanan and V. Shmatikov, "Robust de-anonymization of large sparse datasets," in *Proceedings of the 2008 IEEE Symposium on Security and Privacy*, SP '08, (Washington, DC, USA), pp. 111–125, IEEE Computer Society, 2008.
- [14] W. Shi, N. Li, X. Xie, C. C. Chu, and R. Gadh, "Optimal residential demand response in distribution networks," *IEEE Journal on Selected Areas in Communications*, vol. 32, pp. 1441–1450, July 2014.
- [15] D. Seo, H. Lee, and A. Perrig, "Secure and efficient capability-based power management in the smart grid," in *2011 IEEE Ninth International Symposium on Parallel and Distributed Processing with Applications Workshops*, pp. 119–126, May 2011.
- [16] Y. Gong, Y. Cai, Y. Guo, and Y. Fang, "A privacy-preserving scheme for incentive-based demand response in the smart grid," *IEEE Transactions on Smart Grid*, vol. 7, no. 3, pp. 1304–1313, 2016.
- [17] Z. Zhu, J. Tang, S. Lambotharan, W. H. Chin, and Z. Fan, "An integer linear programming based optimization for home demand-side management in smart grid," in *2012 IEEE PES Innovative Smart Grid Technologies (ISGT)*, pp. 1–5, Jan 2012.
- [18] A. G. Tsikalakis and N. D. Hatziaargyriou, "Centralized control for optimizing microgrids operation," *IEEE Transactions on Energy Conversion*, vol. 23, pp. 241–248, March 2008.
- [19] J. A. P. Lopes, C. L. Moreira, and A. G. Madureira, "Defining control strategies for microgrids islanded operation," *IEEE Transactions on Power Systems*, vol. 21, pp. 916–924, May 2006.
- [20] V. Gulisano, V. Tudor, M. Almgren, and M. Papatriantafyllou, "Bes: Differentially private and distributed event aggregation in advanced metering infrastructures," in *Proceedings of the 2Nd ACM International Workshop on Cyber-Physical System Security*, CPSS '16, (New York, NY, USA), pp. 59–69, ACM, 2016.
- [21] J. M. Bohli, C. Sorge, and O. Ugus, "A privacy model for smart metering," in *2010 IEEE International Conference on Communications Workshops*, pp. 1–5, May 2010.
- [22] X. He, X. Zhang, and C. C. J. Kuo, "A distortion-based approach to privacy-preserving metering in smart grids," *IEEE Access*, vol. 1, pp. 67–78, 2013.
- [23] S. Wang, L. Cui, J. Que, D. H. Choi, X. Jiang, S. Cheng, and L. Xie, "A randomized response model for privacy preserving smart metering," *IEEE Transactions on Smart Grid*, vol. 3, pp. 1317–1324, Sept 2012.
- [24] G. Kalogridis, C. Efthymiou, S. Z. Denic, T. A. Lewis, and R. Cepeda, "Privacy for smart meters: Towards undetectable appliance load signatures," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, pp. 232–237, IEEE, 2010.
- [25] S. McLaughlin, P. McDaniel, and W. Aiello, "Protecting consumer privacy from electric load monitoring," in *Proceedings of the 18th ACM conference on Computer and communications security*, pp. 87–98, ACM, 2011.
- [26] P. Barbosa, A. Brito, and H. Almeida, "A technique to provide differential privacy for appliance usage in smart metering," *Information Sciences*, vol. 370, pp. 355–367, 2016.
- [27] X. Lou, R. Tan, D. Yau, and P. Cheng, "Cost of differential privacy in demand reporting for smart grid economic dispatch," tech. rep., 2016, <http://publish.illinois.edu/cps-security/files/2016/12/dp-cost-techreport.pdf>.
- [28] J. Hsu, A. Roth, T. Roughgarden, and J. Ullman, "Privately solving linear programs," in *International Colloquium on Automata, Languages, and Programming*, pp. 612–624, Springer, 2014.
- [29] W. Shi, X. Xie, C. C. Chu, and R. Gadh, "Distributed optimal energy management in microgrids," *IEEE Transactions on Smart Grid*, vol. 6, pp. 1137–1146, May 2015.
- [30] N. Li, L. Chen, and S. H. Low, "Demand response in radial distribution networks: Distributed algorithm," in *2012 Conference Record of the Forty Sixth Asilomar Conference on Signals, Systems and Computers (ASIOMAR)*, pp. 1549–1553, Nov 2012.
- [31] D. E. Olivares, C. A. Caizares, and M. Kazerani, "A centralized energy management system for isolated microgrids," *IEEE Transactions on Smart Grid*, vol. 5, pp. 1864–1875, July 2014.
- [32] I. Dinur and K. Nissim, "Revealing information while preserving privacy," in *Proceedings of the twenty-second ACM SIGMOD-SIGACT*

SIGART symposium on Principles of database systems, pp. 202–210, ACM, 2003.

- [33] C. Dwork, F. McSherry, K. Nissim, and A. Smith, *Calibrating Noise to Sensitivity in Private Data Analysis*, pp. 265–284. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006.
- [34] A. Blum, K. Ligett, and A. Roth, “A learning theory approach to non-interactive database privacy,” in *Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing*, STOC ’08, (New York, NY, USA), pp. 609–618, ACM, 2008.
- [35] S. P. Kasiviswanathan, H. K. Lee, K. Nissim, S. Raskhodnikova, and A. Smith, “What can we learn privately?,” *SIAM Journal on Computing*, vol. 40, no. 3, pp. 793–826, 2011.
- [36] A. Gupta, K. Ligett, F. McSherry, A. Roth, and K. Talwar, “Differentially private combinatorial optimization,” in *Proceedings of the Twenty-first Annual ACM-SIAM Symposium on Discrete Algorithms*, SODA ’10, (Philadelphia, PA, USA), pp. 1106–1125, Society for Industrial and Applied Mathematics, 2010.
- [37] F. McSherry and K. Talwar, “Mechanism design via differential privacy,” in *Foundations of Computer Science, 2007. FOCS’07. 48th Annual IEEE Symposium on*, pp. 94–103, IEEE, 2007.
- [38] A. Karapetyan, M. Khonji, C. K. Chau, K. Elbassioni, and H. Zeineldin, “Efficient algorithm for scalable event-based demand response management in microgrids,” *IEEE Transactions on Smart Grid*, vol. PP, no. 99, pp. 1–1, 2016.
- [39] K. P. Schneider, Y. Chen, D. P. Chassin, R. Pratt, D. Engel, and S. Thompson, “Modern grid initiative distribution taxonomy final report,” *PNNL-18035, Pacific Northwest National Laboratory, Richland, Washington*, 2008.
- [40] M. E. Baran and F. F. Wu, “Optimal capacitor placement on radial distribution systems,” *IEEE Transactions on Power Delivery*, vol. 4, pp. 725–734, Jan 1989.
- [41] S. H. Low, “Convex relaxation of optimal power flow part i: Formulations and equivalence,” *IEEE Transactions on Control of Network Systems*, vol. 1, pp. 15–27, March 2014.
- [42] L. Gan, N. Li, U. Topcu, and S. H. Low, “Exact convex relaxation of optimal power flow in radial networks,” *IEEE Transactions on Automatic Control*, vol. 60, pp. 72–87, Jan 2015.
- [43] E. Hossain, Z. Han, and H. V. Poor, *Smart grid communications and networking*. Cambridge University Press, 2012.
- [44] C. Dwork, *Differential Privacy: A Survey of Results*, pp. 1–19. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008.